Sicurezza totale

di **Giancarlo Butti**

Guida alla protezione dei beni aziendali

ITER

Giancarlo Butti, *LA BS7799, LA ISO IEC 27001, CRISC, ISM*

Security manager ed auditor presso gruppi bancari, consulente in ambito sicurezza e privacy.

Da sempre affianca all'attività professionale quella di divulgatore tramite articoli, libri, white paper, manuali tecnici, corsi, seminari.

Ha all'attivo oltre 600 articoli e collaborazioni con oltre venti testate (ricoprendo anche il ruolo di redattore tecnico e direttore editoriale); ha pubblicato una quindicina fra libri e white paper alcuni dei quali utilizzati come testi universitari.

Fra i libri pubblicati:

- Lavorare con gli ipertesti, *Gruppo Editoriale Tecniche Nuove* '91 (pp. 200)
- Le procedure contabili informatizzate, *CSB Software* '96 (pp. 140)
- Guida al document management, *Docflow* '97 (pp. 200)
- Discorso sulla multimedialità, *Zecca* '98 (pp. 150)
- Guida al workflow, *Edizioni Domenico Piazza* '99 (pp. 180)
- Internet in azienda, *Zecca* '00 (pp. 150)
- Il protocollo informatico per la pubblica amministrazione, *Maggioli Editore* '03 (coautore)
- Il nuovo Codice Privacy, *Cosmos Service* '04 (pp. 112)

Fra i white paper pubblicati:

- Protocollo informatico a norme AIPA - Guida alle soluzioni basate sulla tecnologia Microsoft, *ITER - Microsoft* '03
- Portali per la pubblica amministrazione, *Microsoft* '04
- Intranet per la pubblica amministrazione, *Microsoft* '04
- Il Codice in materia di protezione dei dati personali (Dlgs 196/03) e le ricadute sui sistemi informatici della Pubblica Amministrazione, *Microsoft* '05 (pp. 140)
- Il Codice in materia di protezione dei dati personali (Dlgs 196/03) e le ricadute sui sistemi informatici della Sanità, *Microsoft* '05 (pp. 140)

Indice

Presentazione

Giancarlo Butti, che ho conosciuto in quanto socio Clusit da diversi anni, si è sempre dimostrato molto attento e sensibile alle problematiche legate alla sicurezza delle informazioni e dal 2003 ad oggi ha realizzato numerose pubblicazione su questi temi.

Con questo volume, che ha come tema la protezione dei beni aziendali, intesi come beni fisici, informazioni e persone, l'autore intende promuovere presso imprenditori e professionisti una giusta percezione dei rischi, proponendo un auto assessment e dando alcuni semplici consigli per elevare da subito il livello della sicurezza.

Non posso che essere riconoscente a Giancarlo per questo sforzo di divulgazione di una corretta cultura della sicurezza delle informazioni, che rientra tra le attività promosse e portate avanti dal Clusit.

Paolo Giudice
Segretario Generale
***CLUSIT** - Associazione Italiana per la Sicurezza Informatica*
www.clusit.it

Prefazione

Negli ultimi anni si è assistito ad una crescente attenzione alla sicurezza. Un termine che esso stesso ha evoluto nel significato, diventando un concetto sempre più pervasivo e parte della vita, personale e professionale, di tutti noi. C'è bisogno di sicurezza quando viaggiamo, quando lavoriamo, quando investiamo il nostro tempo e denaro per costruire il futuro nostro e dei nostri familiari.

Ho conosciuto Giancarlo in occasione di un corso nel quale si parlava di rischi e di gestione del rischio e di come rischio e sicurezza siano strettamente legati: ridurre il rischio e gli effetti potenzialmente negativi è fare sicurezza. Ci siamo trovati in completa sintonia di approccio e di vedute, soprattutto per quanto concerne i rischi incombenti sugli asset aziendali e la necessità di una crescita culturale degli imprenditori e del management delle nostre piccole e medie imprese, che rappresentano il principale tessuto produttivo italiano. Un arcipelago di aziende in possesso di un valore immenso di conoscenza, competenza e beni tangibili.

Qual è però il valore di un bene, tangibile o intangibile che sia? La domanda, apparentemente semplice, ce la poniamo ogni volta che dobbiamo comprarlo, venderlo, dismetterlo, assicurarlo, proteggerlo. Ne stabiliamo il valore ricorrendo alle nostre percezioni, che spesso sono influenzate anche da fattori emotivi. Un oggetto al quale teniamo molto ha un valore che prescinde dal valore effettivo dell'oggetto in sé: la componente emotiva in questo caso è predominante. Compariamo quindi i costi che dovremmo sostenere per proteggerlo con il valore che attribuiamo al nostro oggetto, stabiliamo se sono congrui con il livello di protezione che ci attendiamo e con le nostre possibilità economiche e decidiamo come procedere.

Il processo appena descritto è sostanzialmente analogo ad una Business Impact Analisys: l'impatto, in questo caso, è il nostro "malessere", economico ed emotivo, che ne deriverebbe dalla perdita o danneggiamento. L'analisi, il confronto tra il potenziale (non lo abbiamo ancora perso o danneggiato) "malessere" della perdita o danneggiamento e dal concreto "malessere" dei costi da sostenere per proteggerlo. Normalmente, i due "malesseri" dovrebbero equilibrarsi.

Oggi però sono in campo numerosi aspetti, che fino a pochi anni fa non esistevano ancora, che spostano l'ago della bilancia decisionale: normative, impatti

legali e reputazionali, conseguenze economiche e anche strategiche molto più pressanti.

In altri termini, i beni aziendali vanno molto al di là di quello che rappresentano emozionalmente e normativamente. Le percezioni e le emozioni che prova l'imprenditore nel vedere ciò che ha saputo creare con fatica, capacità e rischio "in proprio" devono cedere il passo ad un approccio alla valutazione dei propri beni più scientifico e razionale e che portino ad una completa consapevolezza di ciò che significano i beni aziendali per il proprio business e per la sopravvivenza e prosperità futura dell'azienda.

Oggi, con l'evoluzione della tecnologia e con lo spostamento del fulcro del valore dagli asset tangibili verso gli asset intangibili (le informazioni, il capitale umano, le conoscenze acquisite negli anni, il marchio ed il valore reputazionale) hanno reso molto più complesso il concetto di sicurezza.

Sicurezza è tutto ciò che salvaguarda, ex-ante ed ex-post, i beni tangibili ed intangibili di un'azienda riducendone i rischi primari (danni diretti agli asset) e secondari (danni indotti a terzi) che incombono su di essi. Le aziende, tuttavia, nascono per produrre beni e servizi, non per "fare" sicurezza.

Oggi, però, non è più possibile produrre e prosperare senza sicurezza. Lo chiedono l'opinione pubblica ed i clienti ed è un vincolo apparente che nasconde grandissime opportunità e può rappresentare un vero e proprio vantaggio competitivo. Vi servireste dei servizi di un'Azienda che "non è sicura" e che quindi potrebbe indurvi un danno o venir meno (senza preavviso) ad un servizio o prodotto per voi essenziale? Probabilmente no. Preferireste volare con una compagnia aerea in linea con i requisiti minimi di sicurezza o con una che dichiaratamente sceglie di offrirne un livello decisamente superiore e ne fa una sua esplicita strategia, anche se ad un prezzo un po' superiore? Probabilmente scegliereste questa seconda.

La sicurezza è qualcosa che oggi, e sempre di più in futuro, costituisce una componente sempre maggiore del valore aggiunto di un prodotto e di un servizio e che il cliente è sempre più propenso a riconoscerlo e a pagarlo. Nel prossimo futuro quei "probabilmente" diventeranno dei "certamente".

Il concetto di sicurezza è legato a doppio filo al concetto di rischio, che, per la mente umana, è di difficile comprensione perché contro intuitivo. Il rischio è qualcosa di aleatorio che è naturalmente incline ad essere respinto. In altri termini, si è propensi a rischiare perché prevale il concetto di privilegiare il certo

(come ad esempio i costi della sicurezza) per l'incerto (un evento che potrebbe accadere, ma che non è ancora accaduto). È sbagliato l'approccio, che va ribaltato di 360°: cosa accadrebbe alla mia azienda se un suo asset venisse danneggiato o perduto? Quel parametro è quello giusto di riferimento, poi – dopo - ne valuto i rischi ai quali è soggetto ed i costi per salvaguardarlo, le implicazioni dirette ed indirette sul business, sulla mia responsabilità di imprenditore e di manager, sulla reputazione dell'azienda sul mercato e sul valore del marchio. Quindi decido: investo per ridurre il rischio o lo accetto, sapendo che comunque, qualunque sia la soluzione che eventualmente adotterò, un po' di incertezza (o rischio residuo) l'avrò sempre. Qualunque sia la decisione, è ponderata e consapevole e l'incertezza è parte del mio rischio imprenditoriale.

Un modo di pensare e di approcciare il rischio e la sicurezza che si può imparare. Anzi, alla luce della crescente attenzione, si deve imparare.

Questo libro non vuole essere un libro per tecnici, ma per imprenditori e manager che vogliono imparare o migliorare il proprio approccio al rischio ed alla sicurezza. Sarà loro utile per far sì che i tecnici in grado di attuare le soluzioni possano lavorare meglio, con risultati migliori ed a costi inferiori.

Fabio Maccafferri
Consulente di Direzione e Partner Pragmatica Consulting
Docente di Informatica e Sistemi Informativi presso l'Università Cattolica
Senior Research Analyst presso il CETIF